IN THE UNITED STATES PATENT & TRADEMARK OFFICE

In re U.S. Utility Patent Application of

CHAREN et al. Art Unit: 2636

Appln. No. 10/767,592 Examiner: Eric Blount

Filed: 28 January 2004

For: LOST PERSON NOTIFICATION SYSTEM

* * *

DECLARATION UNDER 37 CFR 1.131

To The Honorable Commissioner
of Patents and Trademarks
Washington, D.C. 20231

Sir:

I, Art Charen, declare that:

1. I currently reside at 616 Overbrook Road, Baltimore, MD 21212. I have personal knowledge of the facts set forth herein.

2. I am one of the co-inventors of record and co-owner of the above-captioned patent application.

3. I am familiar with the Office Action dated 5 August 2005, which the Patent and Trademark Office mailed in regard to the above-captioned patent application The Examiner rejected all of claims 1-18 under either 35 U.S.C. 102(b) or 103 as being anticipated and/or obvious over Mee (US Publication No. 20040015379), which has a priority date of May 29, 2003.

4. Our present application derives priority from U.S. Provisional Patent Application No. 60/487,552; Filed: July 15, 2003. However, development of our invention as claimed was substantially completed by May 15, 2003. The current invention was fully disclosed by memo dated May 15, 2003 from my co-inventor Robert Glaser to myself (attached). I had asked Mr. Glaser to prepare the memo so

that we could give it to our patent attorney as a basis for our Provisional Patent Application. The memo is written in patent style and explicity details every aspect of our inventon as presently claimed, inclusive of a portable data storage medium containing information related to a child, including an image of the child, to be carried by a parent, a network of kiosks and a system server equipped to receive the data from the portable data storage medium, in the event that the child and the parent are separated. The image of the child is displayed at all kiosks to assist security personnel and bystanders in locating the child. We had previously met with our patent attorney in March of 2003, and upon my receiving the attached memo we immediately turned it over and authorized commencement of the Provisional Patent Application. Our attorneys worked with all due haste and completed the application and filed it on July 15, 2003.

5. I believe that the foregoing showing of facts is such, in character and weight, as to establish reduction to practice prior to the effective date of U.S. Patent Application No. 20040015379 by Mee, as well as conception of the present invention prior to the effective date of the reference coupled with due diligence from prior to said date to a subsequent reduction to practice or to the filing of the current application.

* * * * *

I further declare that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or by both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the above-referenced patent.

Signature: A Charen Date: 10/19/05

Art Charen.

IC Engineering, Inc.
www.ICengineering.com
P.O. Box 321
Owings Mills, MD 21117
410-363-8748

May 15, 2003

CONFIDENTIAL

Art Charen
616 Overbrook Road
Baltimore, MD 21212

Dear Art:

Enclosed is the Watch Guard description we discussed. I have tried to present it as we had discussed; however, as a co-inventor you may wish to modify some of it if you disagree. I am not an attorney, and expect that you will provide this material to an intellectual property (patent) attorney who will prepare the patent application itself. The attorney should change whatever is necessary to best improve the chance of patent approval. The claims are quite important, and normally should be left entirely to the attorney for preparation. I took the liberty of preparing claims myself, but these are merely suggestions to be forwarded to the attorney for consideration. I've provided you with the Word document file so that you and/or the attorney can modify it or export it elsewhere.

The smart cards are about $10; the deposit could be $20 which isn't too unreasonable. The flash drives hold lots more data, but are $17 which I think is a bit high for this application. Here is some background information which could prove helpful to you in marketing the patent should it be approved:

Gemplus Corp. - Main Office Financial & Security Services, Keith Valley Business Center, One Progress Drive, 2nd Floor, Horsham, PA 19044. Contact Mark Friedman (215-390-2487 direct). GemXpresso Pro: Chip size: 64K bytes. Cost is $9.85 in 1000 quantity. GemXpresso RAD III Kit is Gemplus Java Card Development Suite. http://www.gemplus.com/products/gemxpresso_rad_v3_kit/ and http://www.gemplus.com/products/gemxpresso_pro_range/

Schlumberger is another very large smart card manufacturer, 888-343-5773. Maria Nekam 512-331-3394. Amol 512-257-3854.

The 5thSense (tm) Combo Peripheral: $55 in 100 quantity. CONFIRMA-EK Price: $250 software to extract image. Contact: Rich Matthews. Company: Veridicom, Inc., 1248 Reamwood Ave., Sunnyvale CA 94089. Telephone (408) 543-4200, Fax (408) 734-0308, http://www.veridicom.com

ThumbdriveTM Smart: $17 in 1000 quantity for 16M byte device. Company: Trekstor USA Inc., 2411 Old Crow Canyon Rd., Suite 125, San Ramon, CA 94583. Phone: 925 837 4506, Phone: 1888-TREK-199 (1888-8735-199). http://www.trekstorusa.com

Also flash drives from Universal Smart Drive quoted at $18 in 1000 quantity, 888-640-0200 and JM Tek (Julie) $17.25 in 1000 quantity.

Instruments & Equipment Co., 2 Wilson Dr., Sparta, NJ 07871. 800.432.1255. http://www.iepos.com/kiosk/standard-kiosks.html and http://www.iepos.com/kiosk/standard-110spec.html and http://www.iepos.com/kiosk/ncr-ep-45.html

Intel® Pro Video PC Camera: http://www.intel.com/pccamera/provideo/techspec.htm

NETGEAR Inc., 4500 Great America Parkway, Santa Clara, California 95054. Phone: (408) 907-8000 Fax: (408) 907-8097. Web Site: http://www.netgear.com model MR814 WAP http://www.netgear.com/products/details/MR814.asp?view= MA101 802.11b Wireless USB Adapter 500 ft indoor/1500 ft outdoor.

Mako Technologies, 145 N. Swinton Ave., Delray Beach, FL 33444. DT3000 rs-232 smart card reader http://www.mako-tech.com

Sincerely,

Robert E. Glaser

CONFIDENTIAL

Watch Guard

Inventors: Art Charen, 616 Overbrook Rd., Baltimore, MD 21212
Robert E. Glaser, 3213 Patmor Rd., Owings Mills, MD 21117

Abstract

An invention is presented which provides an integrated system to rapidly locate missing children in public and private places. Upon entry to the facility, photographs are taken of each child, and their fingerprints recorded. This information, along with contact data for the children and supervising adults, is stored in a digital memory device which is given to the adult. The information is not recorded in a database or anywhere other than the memory device. When a child becomes missing, the adult inserts the memory device into a nearby kiosk. The kiosk communicates with a central server via wireless means, and the server commands all kiosks on the premises to display the missing child's photographs and to play a siren and voice announcement over public address speakers. Attendants cancel the alert when appropriate. The photographs and the fingerprint scan are available for law enforcement officials should the child not be immediately found. When not in crisis mode, the kiosks are used for general announcements and advertising.

Background of the Invention

Children are susceptible to abduction at public venues. Of particular concern are entertainment complexes, sporting events, and other businesses oriented towards children's activities which operate over a wide area, with multiple exit points. Children can be manipulated or persuaded to make poor decisions which compromise their safety. Experts have reported that children abducted by certain types of perpetrators have a much greater chance of being found alive if they are found within a short period of time. In order to maximize their safety, it is desirable to quickly locate lost children.

Objects of the Invention

The *Watch Guard* invention is a protective device which addresses the problem by providing an integrated system which rapidly makes it known throughout an area that a child is missing, promoting the chance that an abductor will abandon the attempt, and greatly increasing the likelihood of the child being recognized and found quickly by bystanders. The reasoning for the invention is simple: expedite the safe return of the child while the child is likely still in the immediate vicinity – before he or she wanders farther away, is accidentally injured, or is successfully abducted. When activated, Watch Guard immediately alerts everyone in the monitored area of the emergency at strategic locations, and promptly raises the awareness of everyone close by.

Description of the Preferred Embodiment

The preferred embodiment consists of four parts: *an identification card*; a *registration stand*; a *kiosk*; and a *server*. There is one server, one or more registration stands, many kiosks throughout the area, and one identification card per child. The overall system is shown in figure 1, and operates as follows:

1. Upon entry to the facility, children are photographed and fingerprinted. It is imperative that the photographs show the clothing that is being worn on that day to facilitate rapid identification and location. The pictures and fingerprint are taken very rapidly in order to encourage participation in the system.
2. Information is collected from the parent or guardian (referred to subsequently as the *adult*), including the child's and adult's names; address; home telephone number; and the child's and accompanying adult's cellphone numbers if they have wireless telephones with them.

CONFIDENTIAL

3. The above information is digitally stored inside an identification card. The child's name is printed on a label and attached to the identification card. The adult pays a deposit and keeps the identification card.
4. It is important for the public to know that the above information is not stored in a database or in any place except the identification card itself. This gives the adult control of the information, providing confidence that the data will not be misused. Otherwise, privacy-minded individuals might choose not to make use of the system.
5. Under normal circumstances, upon departing the establishment, the adult may return the card, see its contents erased, and retrieve the deposit amount.
6. Should a child be lost, the adult proceeds immediately to a kiosk and inserts and removes the identification card. Immediately, every kiosk displays the photograph of the missing child, and a siren and voice announcement is generated at each kiosk. Only the photograph is shown, and possibly the child's name. The alarm condition remains until an attendant cancels the alarm from the server station.
7. In the event that more than one child is lost at the same time, an adult applies an identification card to a kiosk while an alarm is already in progress. As many such lost children as may occur is handled by having the kiosks rotate between the photographs of each one in succession.
8. It may turn out that simply having the invention deployed at a location causes no abductions to occur, out of fear of apprehension. In such a case, the system has worked by dissuading potential abductors from committing the crime on the premises.
9. In the event that a missing child is not immediately located, the child's photographs and fingerprint image may be given to law enforcement officials to aid in the search.

Detailed descriptions of the system elements follow.

Identification Card

One embodiment of the identification card is a *smart card.* These are credit-card sized devices which contain a microprocessor and nonvolatile read/write memory, referred to as EEPROM (electrically erasable programmable read only memory). They come with standard contacts for use with universal readers; there are also wireless smart cards which do not require physical contact with readers. One example of a contact card which is used in this embodiment is the *GemXpresso Pro* card, manufactured by Gemplus Corporation, of Horsham, PA. Shown in figure 2, this card contains 60K bytes of user programmable EEPROM. This memory is used to store the contact information, photographs, and fingerprint collected at the registration stand. The photographs are read by the kiosks for display.

An alternative embodiment of the identification card is a *Flash Drive*. This device connects to computers via a standard USB socket, and offers read/write flash memory, which is a type of EEPROM. Flash Drives are available in sizes from 8M bytes and up; they can hold a much larger amount of information than smart cards. One example of a Flash Drive is the *Thumbdrive™ Smart*, manufactured by Trekstor USA, of San Ramon, CA. This device, shown in figure 3, contains 16M bytes of storage.

Other forms of digital memory can be used for the identification card, including wireless smart cards, SmartMedia™, CompactFlash™, and PC memory cards. Future larger size versions of Dallas Semiconductor's *iButton* may also prove useful.

Registration Stand

An attended registration stand is located at one or more entrances. The equipment consists of a standard PC (personal computer) and various peripherals: a digital camera; a fingerprint sensor; a smart card reader; a label printer; a keyboard; and video or lcd monitor. These are diagrammed in figure 4. A representative camera is the *Intel® Pro Video PC Camera*. It connects to the PC via a standard USB cable, and its sensor has VGA resolution

(640x480). A representative fingerprint sensor is *The 5thSense™ Combo Peripheral* from Veridicom, of Sunnyvale, CA. It provides 300 by 300 pixels, each an 8 bit gray value (256 shades of gray). This device senses directly from a fingerprint impression, as opposed to other devices which require sliding a finger across the sensor; a contact impression is preferable for applications involving children. The Veridicom part also includes a smart card reader in addition to the fingerprint detector, and connects to the PC via the standard USB port.

A representative self-contained point-of-sale computer is the *NCR EasyPoint™ 45*, from Instruments & Equipment Co., of Sparta, NJ. It includes the necessary keyboard and display, as well as a printer.

In operation, paper forms are provided at the stand, with blanks for the child's and adult's name; address; telephone number; and cellphone numbers, if cellphones are being carried. The adult fills out the form and takes the child to the stand. The attendant has the child press a finger onto the fingerprint sensor, and takes two photos of the child with the camera: a head shot, and a full body shot showing the attire worn. The attendant types the information into the computer from the paper form, and inserts an identification card into the smart card reader. The software in the registration stand computer stores a small text file containing the paper form information, the fingerprint image, and the two photographs of the child into the identification card. It prints a label on the printer with the child's name. The attendant attaches the label to the identification card, collects a deposit fee from the adult, and issues the card to the adult. The identification card can be inserted into the smart card reader and the photographs displayed for verification.

Upon return, the adult may present the identification card to the attendant and have the deposit, or a portion of the deposit, refunded. The attendant issues a command to erase the identification card and removes the attached label. The adult may insert the card into the reader to verify that the personal information has been removed.

The size of the raw fingerprint image is 90K bytes. The software compresses this into a standard JPG format file until it is approximately 15K bytes, which provides a usable image. The full body image is heavily compressed into a standard JPG file of about 14K bytes – image detail is not required, the quality needs to be sufficient only to show the clothing. The image of the child's face is compressed as little as possible, into a JPG file of approximately 30K bytes. Together, the two JPG photo images, the fingerprint JPG image, and a small text file containing the contact information are stored in the GemXpresso Pro card. Standard image processing drivers are used, along with drivers provided in the *CONFIRMA-EK* software development package provided by Veridicom for fingerprint image extraction, and drivers in the *GemXpresso RAD III Development Suite Kit* from Gemplus to interface with their smart card.

When smart cards become available with 128K bytes of EEPROM storage, these will be used for the identification card; this will permit less image compression be done, and provide greater image detail.

For an embodiment using the Thumbdrive™ Smart, or any Flash Drive for the identification card, much more storage is available. This permits storage of the fingerprint image in a raw 90K byte standard GIF format file. The photographs are only slightly compressed for this type of identification card, since there is ample room. Another implementation permits an entire family's group of children be stored in a single Flash Drive; in which case, the kiosks contain numbered buttons to select which child is missing when the Flash Drive identification card is inserted.

Kiosk

Kiosks are placed approximately 100 feet apart so that individuals are never farther than 50 feet from one, and can report a missing child immediately. The floor or ground can be marked by color codes, and clearly visible signs used to designate exactly where to find the nearest kiosk. The kiosk is shown in Figure 5; each consists of: a PC, including an audio card, with display but no keyboard; a smart card reader; a WiFi adapter; a public address amplifier; and a powerhorn (speaker). A representative PC/kiosk is the *110 STEALTH* from Instruments & Equipment Co. A representative smart card reader is model *DT3000* from Mako Technologies, of Delray Beach, FL. It interfaces with the PC via a serial RS-232 cable. A representative WiFi adapter is the *MA101 802.11b Wireless USB Adapter* from Netgear of Santa Clara, CA, which interfaces to the PC's USB port. A representative public address amplifier is model *#32-2001 20W Public Address Amplifier* from Radio Shack. A representative powerhorn is model *#40-1440 Indoor/Outdoor Powerhorn* from Radio Shack.

The PC software detects the insertion of an identification card into the smart card reader. It retrieves all of the information stored in the card, and transmits it to the server via the WiFi adapter. WiFi, or 802.11b, is a standard wireless protocol used for LAN's (local area networks). It includes encryption protocols for security purposes. The server receives the information from its WAP (wireless access point) and immediately broadcasts to all kiosks, from its WAP to the kiosk WiFi adapters. The broadcast contains the two photographs of the missing child and the child's name, and an instruction to display the information and activate a siren alarm and voice announcement.

Each kiosk begins displaying the missing child's photographs and possibly the child's name. The PC has stored on its hard drive a standard format WAV file which is a siren sound. It also has an audio recording in the same format which states "Please be on the lookout for a missing child, whose photograph is on the monitor," or similar. The PC proceeds to repetitively play the siren and announcement WAV sounds interspersed. The PC's audio card output is connected to the public address amplifier; and the amplifier's output is connected to the powerhorn. The immediate area surrounding the kiosk is alerted with the siren and announcement, drawing attention to the pictures of the missing child.

Should the kiosks report additional children missing, the server alerts the kiosks to rotate the display between photographs of each missing child, and to change the announcement to one which states that several children are missing.

The kiosk continues to display the photographs and make the announcement until the server instructs it to halt. During periods when no alert is in progress, the kiosk may display special events, sale items, food specials, etc., as transmitted from the server.

Server

The server, shown in figure 6, consists of a PC with keyboard and a wireless access point (WAP) device. A representative WAP is the *MR814 WAP* from Netgear, which interfaces to the PC's USB port. The server controls the wireless LAN, and basically listens for transmissions from the kiosks reporting that an identification card has been inserted to alert of a missing child. Upon receipt of such information, it relays the child's photographs and name to each kiosk, and commands the kiosks to activate the alert siren, announcement, and to display the photographs. The outdoor range of the WAP is approximately 1500 feet; in the event that a kiosk is farther than this distance, and is unable to communicate with the server, one or more of the kiosks are equipped with additional WAP devices to relay communications from the server.

During an alert, the server displays the relevant contact information and identifies the location of the kiosk reporting the missing child. An authorized attendant can control the process by instructing the server to end crisis mode; when this occurs, the server transmits instructions to the kiosks to return to normal operation.

In practice, the server is incorporated into one of the registration stands. This only requires the MR814 WAP peripheral be added to the NCR EasyPoint™ 45 PC used at the registration stand. Separate software applications independently control the registration stand and server functions.

Claims

The embodiment depicted uses smart cards as identification cards; other digital media devices can be used as well. Analog means can also be used, but digital means are preferable in the modern day environment. The embodiment shown uses a wireless LAN to connect the kiosks with the server; standard wired LAN and powerline data means can also be used for such purposes. Having described several embodiments of a new and improved child safety alert system, it is believed that other modifications, variations, and changes will be suggested to those skilled in the art in the light of the above teachings. It is, therefore, to be understood that all such variations, modifications, and changes are believed to come within the scope of the invention as defined by the appended claims.

What is claimed is:

1. A premise alert system consisting of identification cards, one or more registration stations, multiple kiosks, and a server, wherein the registration station collects identifying information and stores it in identification cards, the kiosks retrieve information from identification cards and transmit that information to the server, and the server transmits that information and commands to each of the kiosks.
2. A premise alert system according to claim 1 which provides for rapid collection of photographs at registration stations.
3. A premise alert system according to claim 1 which provides for rapid collection of fingerprint images at registration stations.
4. A premise alert system according to claim 1 which provides for rapid collection of photographs and fingerprint images at registration stations.
5. A premise alert system according to claim 1 which protects children.
6. A premise alert system according to claim 1 which protects the mentally disabled.
7. A premise alert system according to claim 1 which uses digital memory devices for the identification cards.
8. A premise alert system according to claim 1 wherein the registration station consists of a computer and a digital camera.
9. A premise alert system according to claim 1 wherein the registration station consists of a computer and a fingerprint scanner.
10. A premise alert system according to claim 1 wherein the registration station consists of a computer and a digital memory reader.
11. A premise alert system according to claim 1 wherein the registration station consists of a computer, a digital camera, and a fingerprint scanner.
12. A premise alert system according to claim 1 wherein the registration station consists of a computer, a digital camera, and a digital memory reader.
13. A premise alert system according to claim 1 wherein the registration station consists of a computer, a fingerprint scanner, and a digital memory reader.
14. A premise alert system according to claim 1 wherein the registration station consists of a computer, a digital camera, a fingerprint scanner, and a digital memory reader.
15. A premise alert system according to claim 1, an identification card according to claim 7, and a registration station according to claims 10, 12, 13, or 14 wherein the digital memory reader consists of a smart card reader.
16. A premise alert system according to claim 1 wherein the kiosks and server are connected by a network.
17. A premise alert system according to claim 1, and kiosks and a server according to claim 16, wherein the network means is wired.

18. A premise alert system according to claim 1, and kiosks and a server according to claim 17, wherein the network means is data over powerline.
19. A premise alert system according to claim 1, and kiosks and a server according to claim 16, wherein the network means is wireless.
20. A premise alert system according to claim 1, and kiosks and a server according to claim 19, wherein the wireless network meets the 802.11a standard.
21. A premise alert system according to claim 1, and kiosks and a server according to claim 19, wherein the wireless network meets the 802.11b standard.
22. A premise alert system according to claim 1, and kiosks and a server according to claim 19, wherein the wireless network meets the 802.11g standard.
23. A premise alert system according to claim 1 wherein the kiosk consists of a computer and video display.
24. A premise alert system according to claim 1 wherein the kiosk consists of a computer and lcd display.
25. A premise alert system according to claim 1, and a kiosk according to claim 23 or 24, wherein the kiosk contains a public address amplifier and speaker.
26. A premise alert system according to claim 1, and a kiosk according to claim 23, 24, or 25, wherein the kiosk contains a digital memory reader.
27. A premise alert system according to claim 1, and a kiosk according to claim 26, wherein the digital memory reader is a smart card reader.
28. A premise alert system according to claim 1, and a kiosk according to claim 23, 24, 25, 26, or 27, wherein the kiosk utilizes a network according to claim 16, 17, 18, 19, 20, 21, or 22.
29. A premise alert system according to claim 1, and a server consisting of a computer and network interface according to claim 16, 17, 18, 19, 20, 21, or 22.
30. A premise alert system according to claim 1 wherein identifying information is not stored in a database.
31. A premise alert system according to claim 1 wherein identifying information is stored in a database.

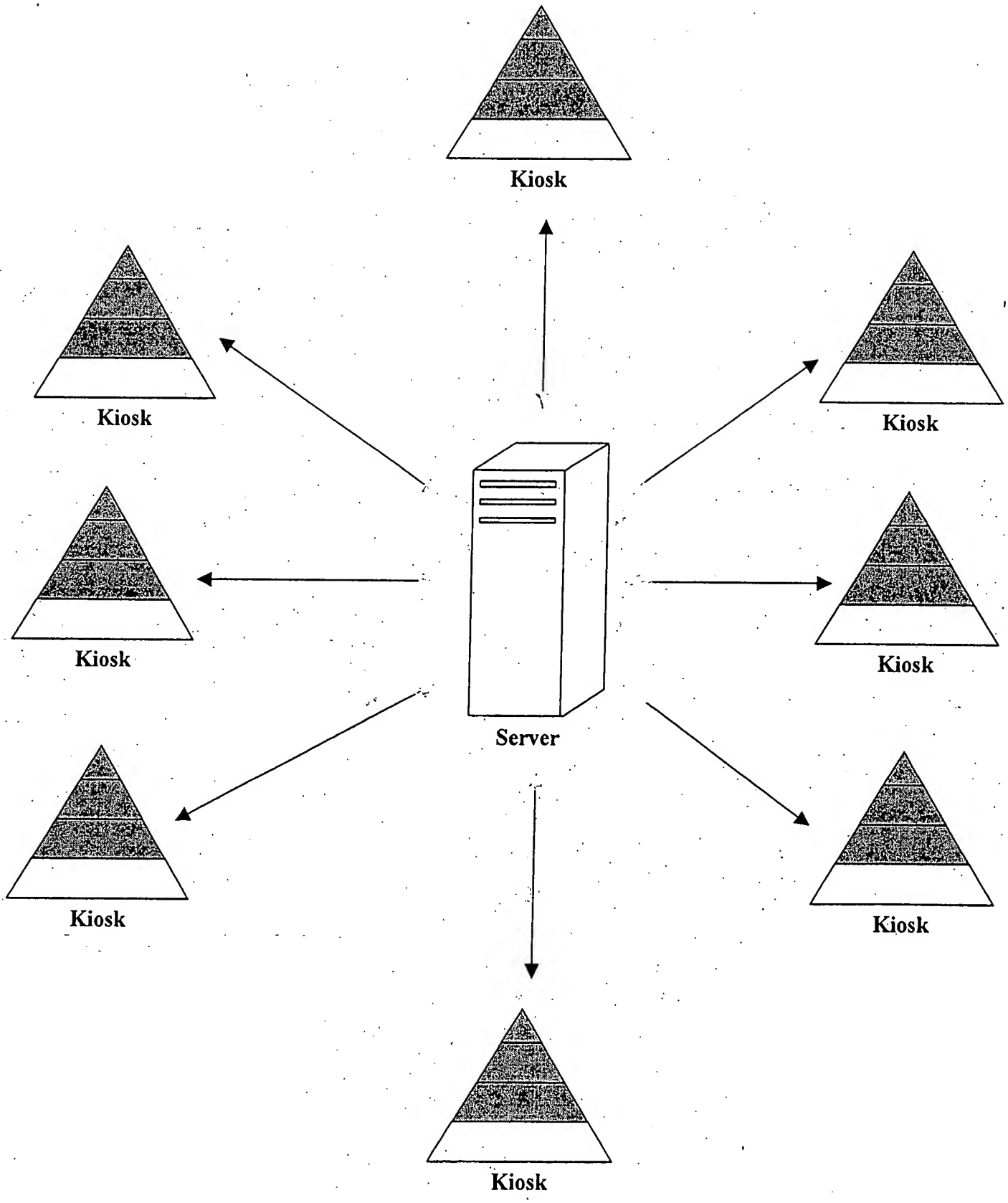


Figure 1: System Diagram

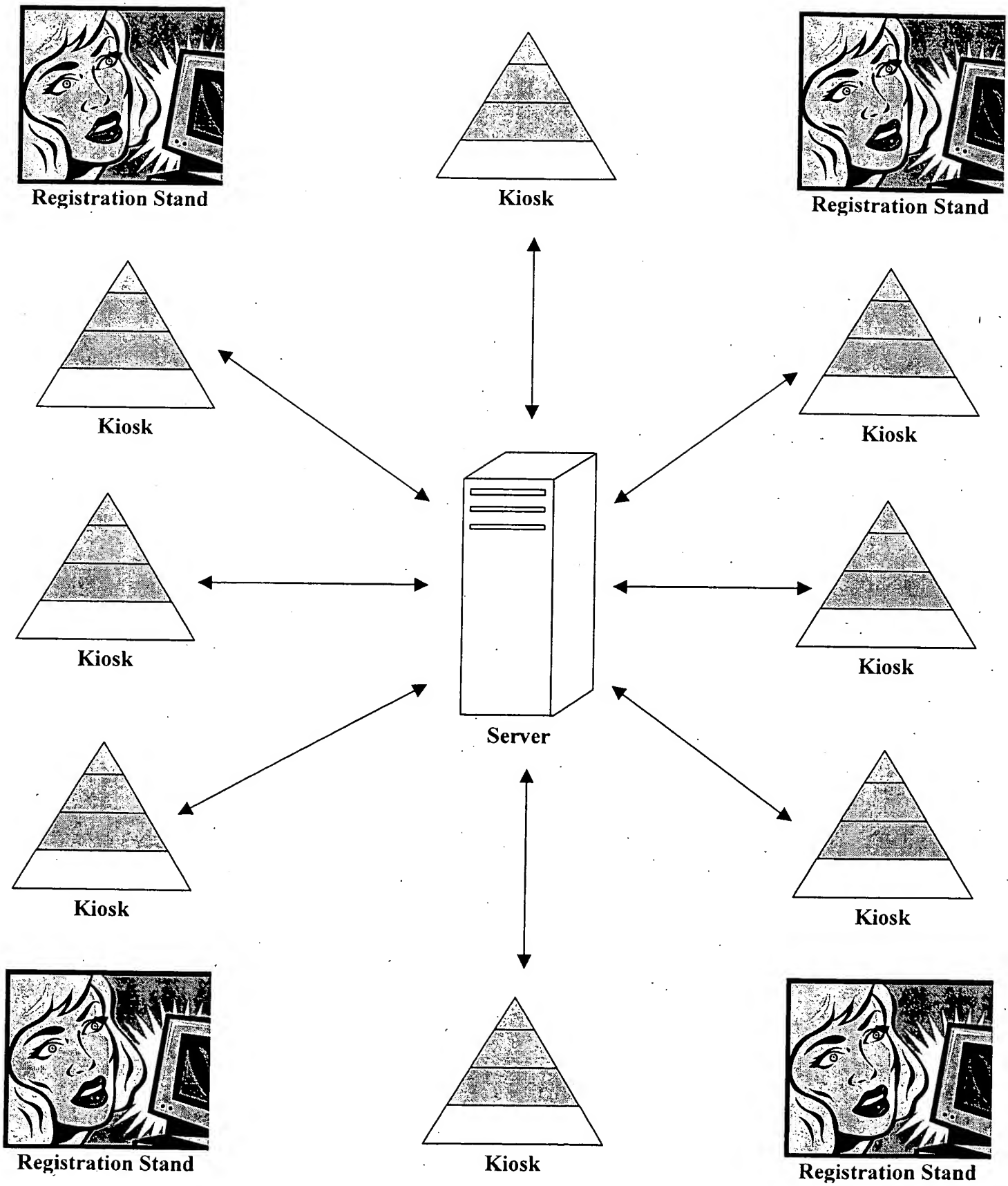


Figure 1: System Diagram

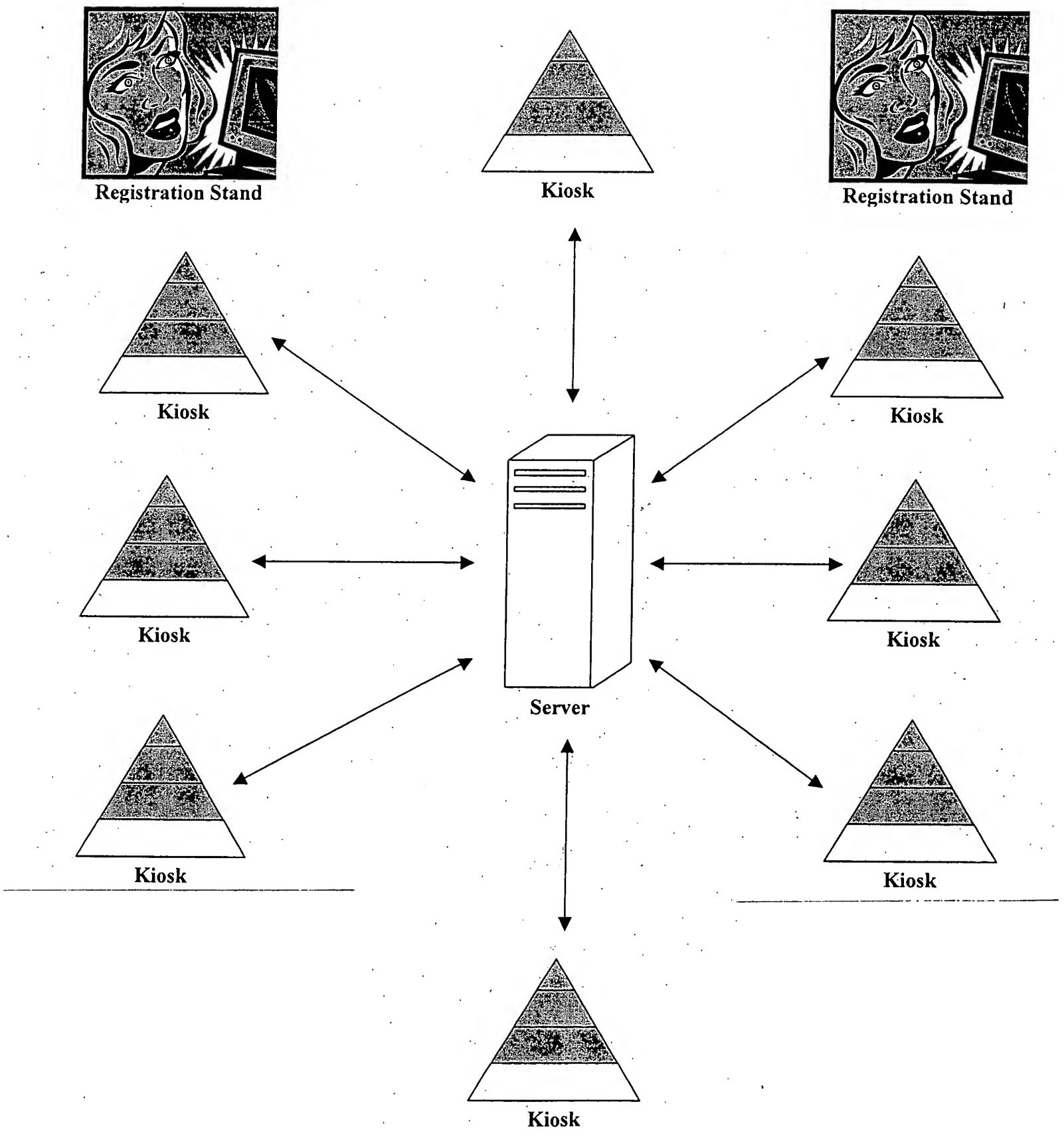
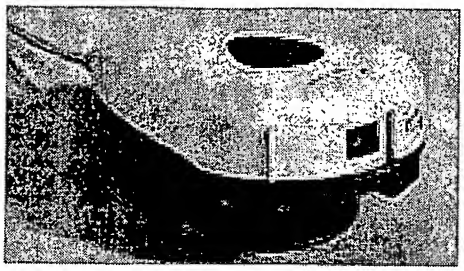


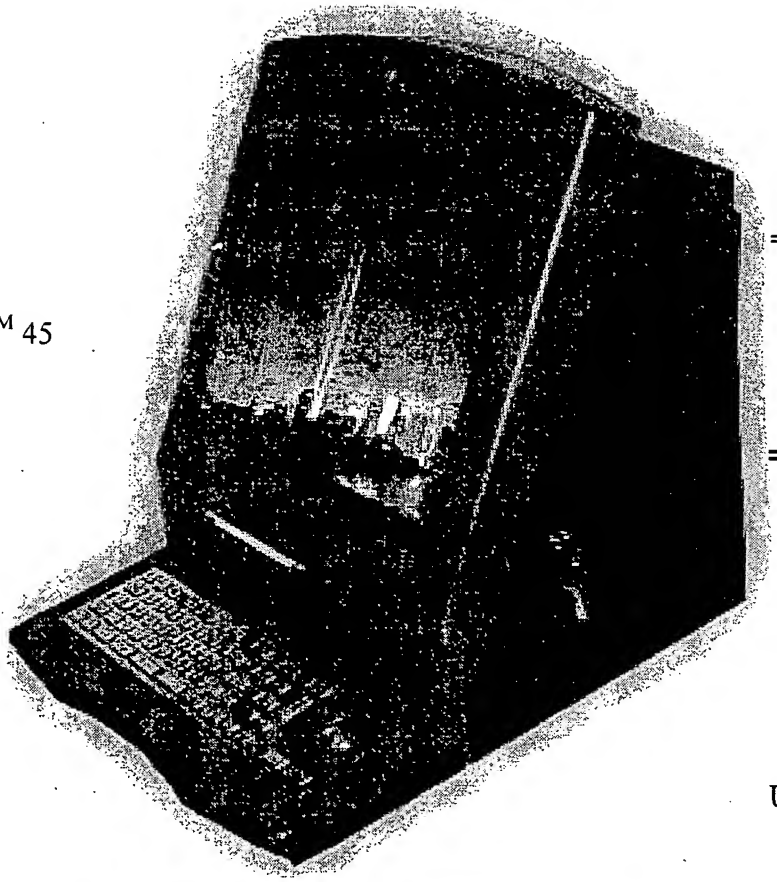
Figure 1: System Diagram

Pro Video PC Camera



USB Cable

NCR EasyPoint™ 45



USB Cable

The 5thSense™
Combo Peripheral

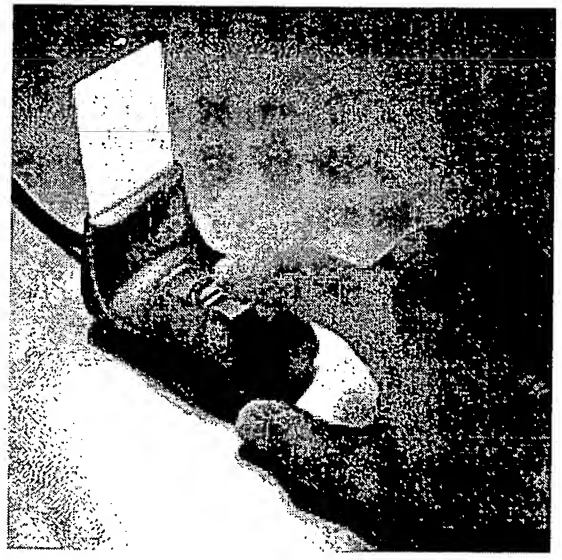
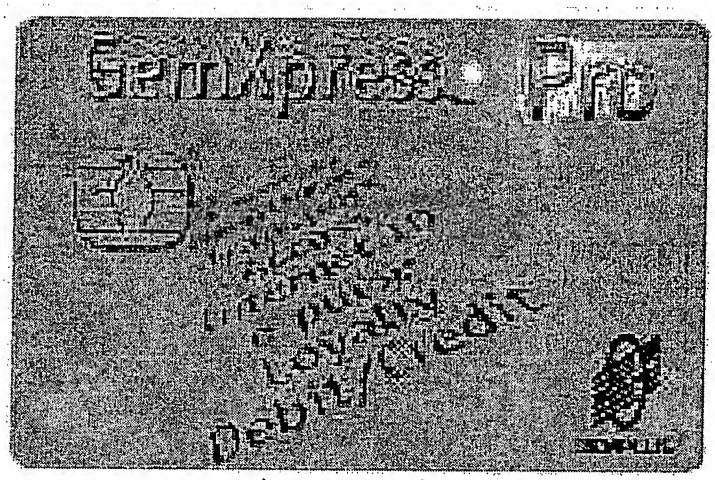
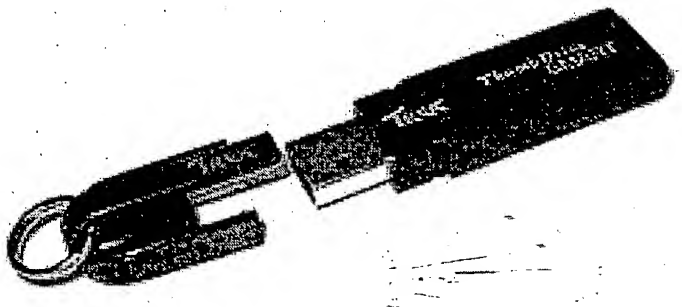


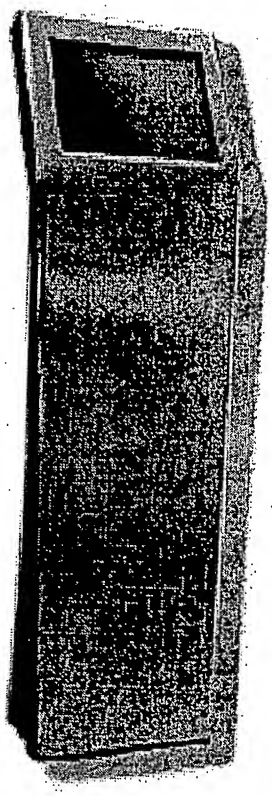
Figure 4: Registration Stand



Figure



Figure



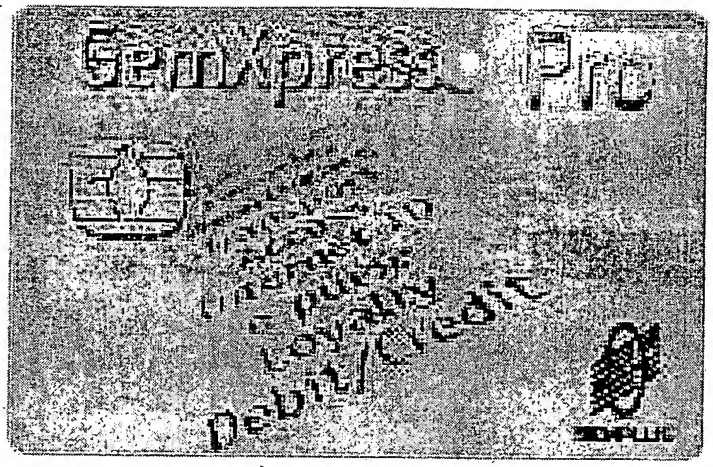


Figure 2: GemXpresso Pro Smart Card

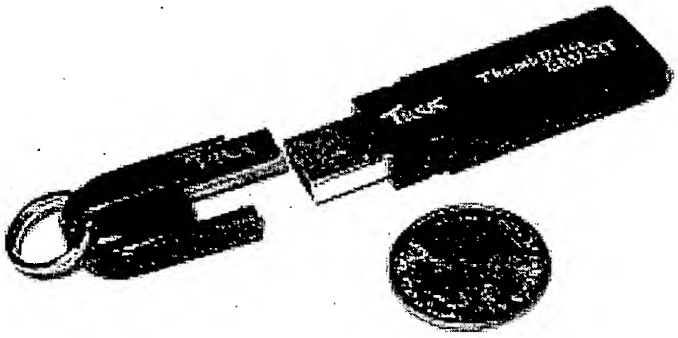


Figure 3: Thumbdrive™ Smart

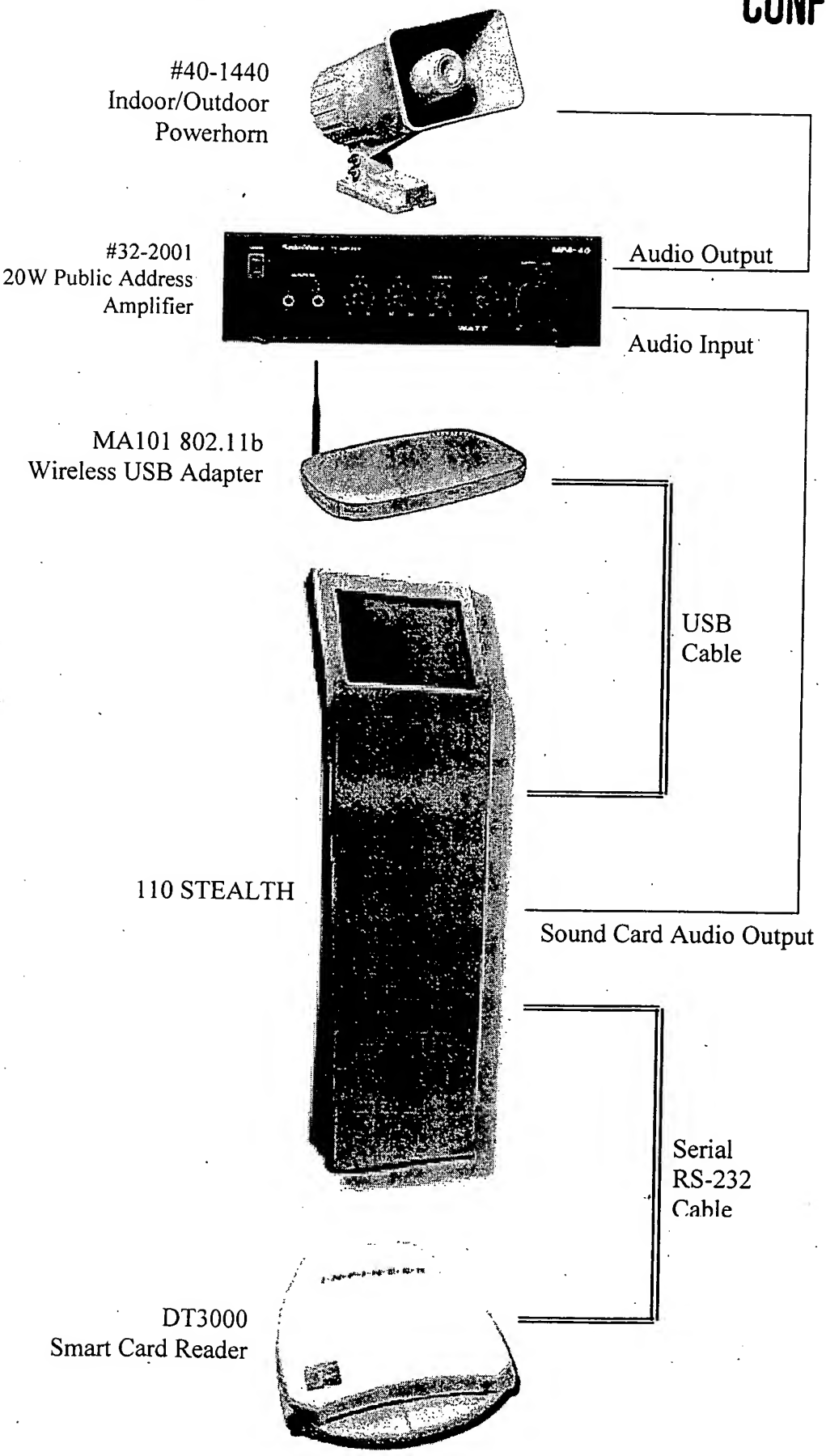


Figure 5: Kiosk

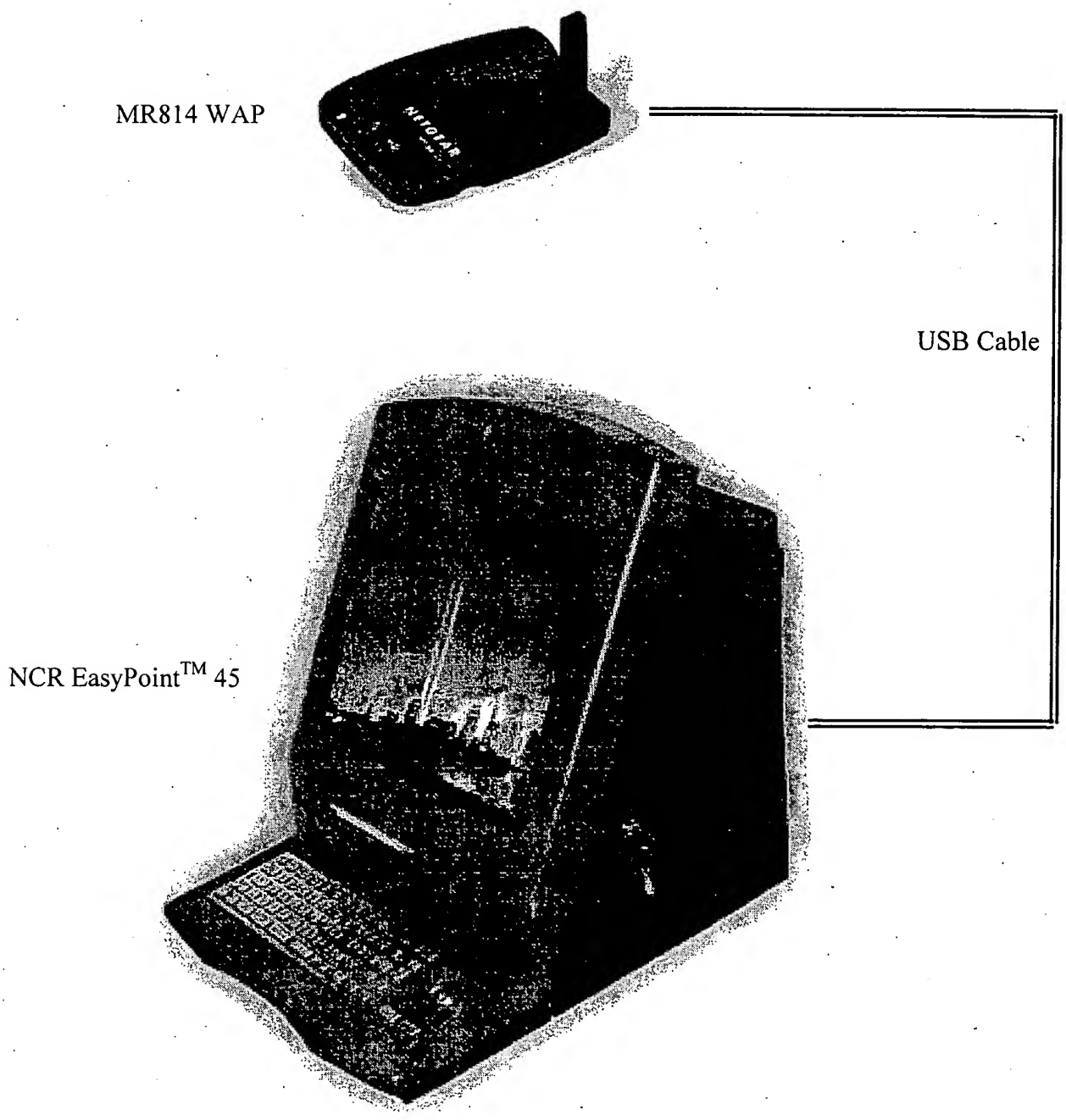


Figure 6: Server

CONFIDENTIAL

Watch Guard

Inventors: Art Charen, 616 Overbrook Rd., Baltimore, MD 21212
Robert E. Glaser, 3213 Patmor Rd., Owings Mills, MD 21117

Abstract

An invention is presented which provides an integrated system to rapidly locate missing children in public and private places. Upon entry to the facility, photographs are taken of each child, and their fingerprints recorded. This information, along with contact data for the children and supervising adults, is stored in a digital memory device which is given to the adult. The information is not recorded in a database or anywhere other than the memory device. When a child becomes missing, the adult inserts the memory device into a nearby kiosk. The kiosk communicates with a central server via wireless means, and the server commands all kiosks on the premises to display the missing child's photographs and to play a siren and voice announcement over public address speakers. Attendants cancel the alert when appropriate. The photographs and the fingerprint scan are available for law enforcement officials should the child not be immediately found. When not in crisis mode, the kiosks are used for general announcements and advertising.

Background of the Invention

Children are susceptible to abduction at public venues. Of particular concern are entertainment complexes, sporting events, and other businesses oriented towards children's activities which operate over a wide area, with multiple exit points. Children can be manipulated or persuaded to make poor decisions which compromise their safety. Experts have reported that children abducted by certain types of perpetrators have a much greater chance of being found alive if they are found within a short period of time. In order to maximize their safety, it is desirable to quickly locate lost children.

Objects of the Invention

The *Watch Guard* invention is a protective device which addresses the problem by providing an integrated system which rapidly makes it known throughout an area that a child is missing, promoting the chance that an abductor will abandon the attempt, and greatly increasing the likelihood of the child being recognized and found quickly by bystanders. The reasoning for the invention is simple: expedite the safe return of the child while the child is likely still in the immediate vicinity – before he or she wanders farther away, is accidentally injured, or is successfully abducted. When activated, Watch Guard immediately alerts everyone in the monitored area of the emergency at strategic locations, and promptly raises the awareness of everyone close by.

Description of the Preferred Embodiment

The preferred embodiment consists of four parts: *an identification card*; a *registration stand*; a *kiosk*; and a *server*. There is one server, one or more registration stands, many kiosks throughout the area, and one identification card per child. The overall system is shown in figure 1, and operates as follows:

1. Upon entry to the facility, children are photographed and fingerprinted. It is imperative that the photographs show the clothing that is being worn on that day to facilitate rapid identification and location. The pictures and fingerprint are taken very rapidly in order to encourage participation in the system.
2. Information is collected from the parent or guardian (referred to subsequently as the *adult*), including the child's and adult's names; address; home telephone number; and the child's and accompanying adult's cellphone numbers if they have wireless telephones with them.

3. The above information is digitally stored inside an identification card. The child's name is printed on a label and attached to the identification card. The adult pays a deposit and keeps the identification card.
4. It is important for the public to know that the above information is not stored in a database or in any place except the identification card itself. This gives the adult control of the information, providing confidence that the data will not be misused. Otherwise, privacy-minded individuals might choose not to make use of the system.
5. Under normal circumstances, upon departing the establishment, the adult may return the card, see its contents erased, and retrieve the deposit amount.
6. Should a child be lost, the adult proceeds immediately to a kiosk and inserts and removes the identification card. Immediately, every kiosk displays the photograph of the missing child, and a siren and voice announcement is generated at each kiosk. Only the photograph is shown, and possibly the child's name. The alarm condition remains until an attendant cancels the alarm from the server station.
7. In the event that more than one child is lost at the same time, an adult applies an identification card to a kiosk while an alarm is already in progress. As many such lost children as may occur is handled by having the kiosks rotate between the photographs of each one in succession.
8. It may turn out that simply having the invention deployed at a location causes no abductions to occur, out of fear of apprehension. In such a case, the system has worked by dissuading potential abductors from committing the crime on the premises.
9. In the event that a missing child is not immediately located, the child's photographs and fingerprint image may be given to law enforcement officials to aid in the search.

Detailed descriptions of the system elements follow.

Identification Card

One embodiment of the identification card is a *smart card.* These are credit-card sized devices which contain a microprocessor and nonvolatile read/write memory, referred to as EEPROM (electrically erasable programmable read only memory). They come with standard contacts for use with universal readers; there are also wireless smart cards which do not require physical contact with readers. One example of a contact card which is used in this embodiment is the *GemXpresso Pro* card, manufactured by Gemplus Corporation, of Horsham, PA. Shown in figure 2, this card contains 60K bytes of user programmable EEPROM. This memory is used to store the contact information, photographs, and fingerprint collected at the registration stand. The photographs are read by the kiosks for display.

An alternative embodiment of the identification card is a *Flash Drive.* This device connects to computers via a standard USB socket, and offers read/write flash memory, which is a type of EEPROM. Flash Drives are available in sizes from 8M bytes and up; they can hold a much larger amount of information than smart cards. One example of a Flash Drive is the *Thumbdrive™ Smart*, manufactured by Trekstor USA, of San Ramon, CA. This device, shown in figure 3, contains 16M bytes of storage.

Other forms of digital memory can be used for the identification card, including wireless smart cards, SmartMedia™, CompactFlash™, and PC memory cards. Future larger size versions of Dallas Semiconductor's *iButton* may also prove useful.

Registration Stand

An attended registration stand is located at one or more entrances. The equipment consists of a standard PC (personal computer) and various peripherals: a digital camera; a fingerprint sensor; a smart card reader; a label printer; a keyboard; and video or lcd monitor. These are diagrammed in figure 4. A representative camera is the *Intel® Pro Video PC Camera.* It connects to the PC via a standard USB cable, and its sensor has VGA resolution

(640x480). A representative fingerprint sensor is *The 5thSense™ Combo Peripheral* from Veridicom, of Sunnyvale, CA. It provides 300 by 300 pixels, each an 8 bit gray value (256 shades of gray). This device senses directly from a fingerprint impression, as opposed to other devices which require sliding a finger across the sensor; a contact impression is preferable for applications involving children. The Veridicom part also includes a smart card reader in addition to the fingerprint detector, and connects to the PC via the standard USB port.

A representative self-contained point-of-sale computer is the *NCR EasyPoint™ 45*, from Instruments & Equipment Co., of Sparta, NJ. It includes the necessary keyboard and display, as well as a printer.

In operation, paper forms are provided at the stand, with blanks for the child's and adult's name; address; telephone number; and cellphone numbers, if cellphones are being carried. The adult fills out the form and takes the child to the stand. The attendant has the child press a finger onto the fingerprint sensor, and takes two photos of the child with the camera: a head shot, and a full body shot showing the attire worn. The attendant types the information into the computer from the paper form, and inserts an identification card into the smart card reader. The software in the registration stand computer stores a small text file containing the paper form information, the fingerprint image, and the two photographs of the child into the identification card. It prints a label on the printer with the child's name. The attendant attaches the label to the identification card, collects a deposit fee from the adult, and issues the card to the adult. The identification card can be inserted into the smart card reader and the photographs displayed for verification.

Upon return, the adult may present the identification card to the attendant and have the deposit, or a portion of the deposit, refunded. The attendant issues a command to erase the identification card and removes the attached label. The adult may insert the card into the reader to verify that the personal information has been removed.

The size of the raw fingerprint image is 90K bytes. The software compresses this into a standard JPG format file until it is approximately 15K bytes, which provides a usable image. The full body image is heavily compressed into a standard JPG file of about 14K bytes – image detail is not required, the quality needs to be sufficient only to show the clothing. The image of the child's face is compressed as little as possible, into a JPG file of approximately 30K bytes. Together, the two JPG photo images, the fingerprint JPG image, and a small text file containing the contact information are stored in the GemXpresso Pro card. Standard image processing drivers are used, along with drivers provided in the *CONFIRMA-EK* software development package provided by Veridicom for fingerprint image extraction, and drivers in the *GemXpresso RAD III Development Suite Kit* from Gemplus to interface with their smart card.

When smart cards become available with 128K bytes of EEPROM storage, these will be used for the identification card; this will permit less image compression be done, and provide greater image detail.

For an embodiment using the Thumbdrive™ Smart, or any Flash Drive for the identification card, much more storage is available. This permits storage of the fingerprint image in a raw 90K byte standard GIF format file. The photographs are only slightly compressed for this type of identification card, since there is ample room. Another implementation permits an entire family's group of children be stored in a single Flash Drive; in which case, the kiosks contain numbered buttons to select which child is missing when the Flash Drive identification card is inserted.

Kiosk

Kiosks are placed approximately 100 feet apart so that individuals are never farther than 50 feet from one, and can report a missing child immediately. The floor or ground can be marked by color codes, and clearly visible signs used to designate exactly where to find the nearest kiosk. The kiosk is shown in Figure 5; each consists of: a PC, including an audio card, with display but no keyboard; a smart card reader; a WiFi adapter; a public address amplifier; and a powerhorn (speaker). A representative PC/kiosk is the *110 STEALTH* from Instruments & Equipment Co. A representative smart card reader is model *DT3000* from Mako Technologies, of Delray Beach, FL. It interfaces with the PC via a serial RS-232 cable. A representative WiFi adapter is the *MA101 802.11b Wireless USB Adapter* from Netgear of Santa Clara, CA, which interfaces to the PC's USB port. A representative public address amplifier is model *#32-2001 20W Public Address Amplifier* from Radio Shack. A representative powerhorn is model *#40-1440 Indoor/Outdoor Powerhorn* from Radio Shack.

The PC software detects the insertion of an identification card into the smart card reader. It retrieves all of the information stored in the card, and transmits it to the server via the WiFi adapter. WiFi, or 802.11b, is a standard wireless protocol used for LAN's (local area networks). It includes encryption protocols for security purposes. The server receives the information from its WAP (wireless access point) and immediately broadcasts to all kiosks, from its WAP to the kiosk WiFi adapters. The broadcast contains the two photographs of the missing child and the child's name, and an instruction to display the information and activate a siren alarm and voice announcement.

Each kiosk begins displaying the missing child's photographs and possibly the child's name. The PC has stored on its hard drive a standard format WAV file which is a siren sound. It also has an audio recording in the same format which states "Please be on the lookout for a missing child, whose photograph is on the monitor," or similar. The PC proceeds to repetitively play the siren and announcement WAV sounds interspersed. The PC's audio card output is connected to the public address amplifier; and the amplifier's output is connected to the powerhorn. The immediate area surrounding the kiosk is alerted with the siren and announcement, drawing attention to the pictures of the missing child.

Should the kiosks report additional children missing, the server alerts the kiosks to rotate the display between photographs of each missing child, and to change the announcement to one which states that several children are missing.

The kiosk continues to display the photographs and make the announcement until the server instructs it to halt. During periods when no alert is in progress, the kiosk may display special events, sale items, food specials, etc., as transmitted from the server.

Server

The server, shown in figure 6, consists of a PC with keyboard and a wireless access point (WAP) device. A representative WAP is the *MR814 WAP* from Netgear, which interfaces to the PC's USB port. The server controls the wireless LAN, and basically listens for transmissions from the kiosks reporting that an identification card has been inserted to alert of a missing child. Upon receipt of such information, it relays the child's photographs and name to each kiosk, and commands the kiosks to activate the alert siren, announcement, and to display the photographs. The outdoor range of the WAP is approximately 1500 feet; in the event that a kiosk is farther than this distance, and is unable to communicate with the server, one or more of the kiosks are equipped with additional WAP devices to relay communications from the server.

During an alert, the server displays the relevant contact information and identifies the location of the kiosk reporting the missing child. An authorized attendant can control the process by instructing the server to end crisis mode; when this occurs, the server transmits instructions to the kiosks to return to normal operation.

In practice, the server is incorporated into one of the registration stands. This only requires the MR814 WAP peripheral be added to the NCR EasyPoint™ 45 PC used at the registration stand. Separate software applications independently control the registration stand and server functions.

Claims

The embodiment depicted uses smart cards as identification cards; other digital media devices can be used as well. Analog means can also be used, but digital means are preferable in the modern day environment. The embodiment shown uses a wireless LAN to connect the kiosks with the server; standard wired LAN and powerline data means can also be used for such purposes. Having described several embodiments of a new and improved child safety alert system, it is believed that other modifications, variations, and changes will be suggested to those skilled in the art in the light of the above teachings. It is, therefore, to be understood that all such variations, modifications, and changes are believed to come within the scope of the invention as defined by the appended claims.

What is claimed is:

1. A premise alert system consisting of identification cards, one or more registration stations, multiple kiosks, and a server, wherein the registration station collects identifying information and stores it in identification cards, the kiosks retrieve information from identification cards and transmit that information to the server, and the server transmits that information and commands to each of the kiosks.
2. A premise alert system according to claim 1 which provides for rapid collection of photographs at registration stations.
3. A premise alert system according to claim 1 which provides for rapid collection of fingerprint images at registration stations.
4. A premise alert system according to claim 1 which provides for rapid collection of photographs and fingerprint images at registration stations.
5. A premise alert system according to claim 1 which protects children.
6. A premise alert system according to claim 1 which protects the mentally disabled.
7. A premise alert system according to claim 1 which uses digital memory devices for the identification cards.
8. A premise alert system according to claim 1 wherein the registration station consists of a computer and a digital camera.
9. A premise alert system according to claim 1 wherein the registration station consists of a computer and a fingerprint scanner.
10. A premise alert system according to claim 1 wherein the registration station consists of a computer and a digital memory reader.
11. A premise alert system according to claim 1 wherein the registration station consists of a computer, a digital camera, and a fingerprint scanner.
12. A premise alert system according to claim 1 wherein the registration station consists of a computer, a digital camera, and a digital memory reader.
13. A premise alert system according to claim 1 wherein the registration station consists of a computer, a fingerprint scanner, and a digital memory reader.
14. A premise alert system according to claim 1 wherein the registration station consists of a computer, a digital camera, a fingerprint scanner, and a digital memory reader.
15. A premise alert system according to claim 1, an identification card according to claim 7, and a registration station according to claims 10, 12, 13, or 14 wherein the digital memory reader consists of a smart card reader.
16. A premise alert system according to claim 1 wherein the kiosks and server are connected by a network.
17. A premise alert system according to claim 1, and kiosks and a server according to claim 16, wherein the network means is wired.

18. A premise alert system according to claim 1, and kiosks and a server according to claim 17, wherein the network means is data over powerline.
19. A premise alert system according to claim 1, and kiosks and a server according to claim 16, wherein the network means is wireless.
20. A premise alert system according to claim 1, and kiosks and a server according to claim 19, wherein the wireless network meets the 802.11a standard.
21. A premise alert system according to claim 1, and kiosks and a server according to claim 19, wherein the wireless network meets the 802.11b standard.
22. A premise alert system according to claim 1, and kiosks and a server according to claim 19, wherein the wireless network meets the 802.11g standard.
23. A premise alert system according to claim 1 wherein the kiosk consists of a computer and video display.
24. A premise alert system according to claim 1 wherein the kiosk consists of a computer and lcd display.
25. A premise alert system according to claim 1, and a kiosk according to claim 23 or 24, wherein the kiosk contains a public address amplifier and speaker.
26. A premise alert system according to claim 1, and a kiosk according to claim 23, 24, or 25, wherein the kiosk contains a digital memory reader.
27. A premise alert system according to claim 1, and a kiosk according to claim 26, wherein the digital memory reader is a smart card reader.
28. A premise alert system according to claim 1, and a kiosk according to claim 23, 24, 25, 26, or 27, wherein the kiosk utilizes a network according to claim 16, 17, 18, 19, 20, 21, or 22.
29. A premise alert system according to claim 1, and a server consisting of a computer and network interface according to claim 16, 17, 18, 19, 20, 21, or 22.
30. A premise alert system according to claim 1 wherein identifying information is not stored in a database.
31. A premise alert system according to claim 1 wherein identifying information is stored in a database.

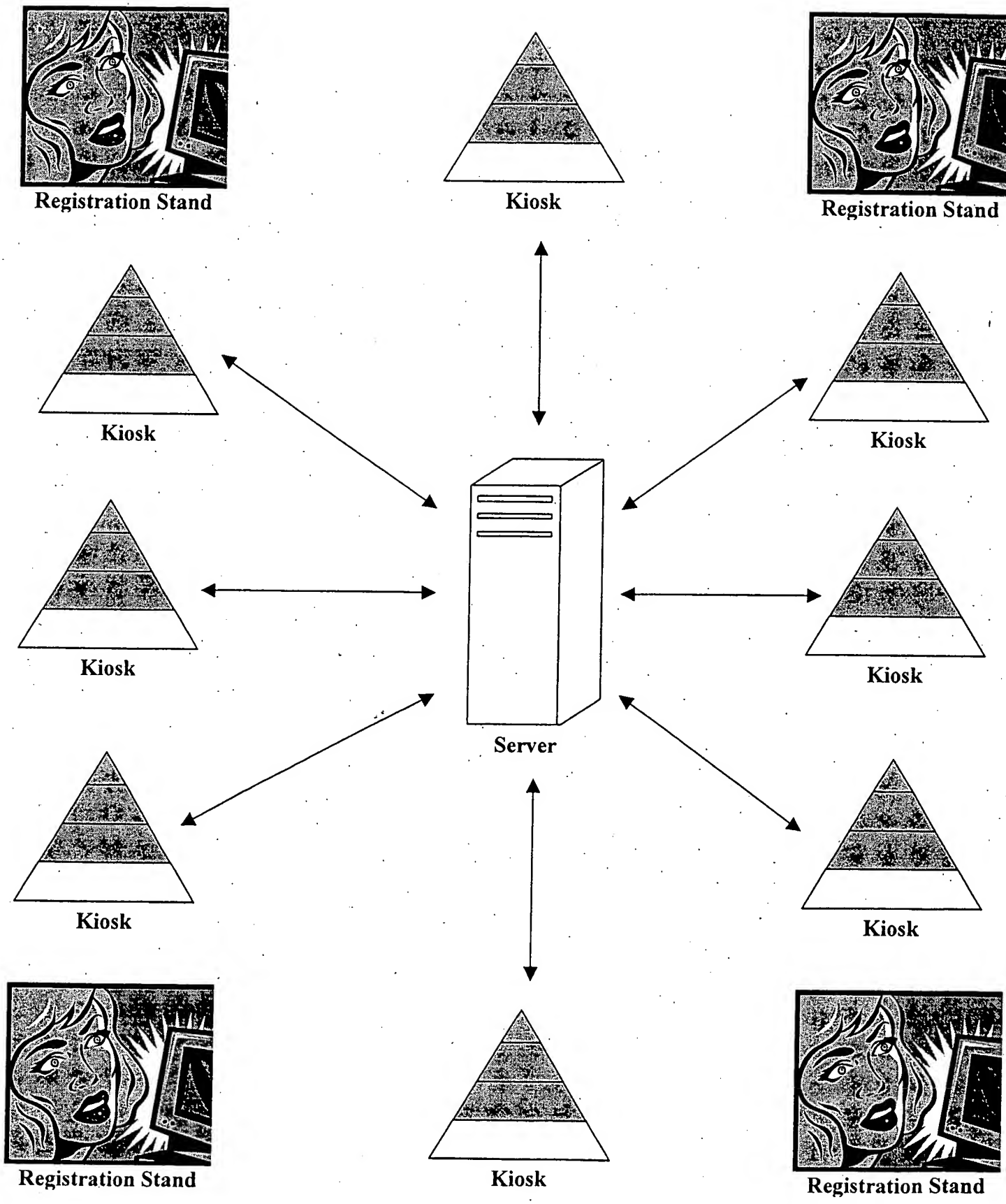


Figure 1: System Diagram